



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/637,229	08/11/2000	Cetin K. Koc	245-55512	7362

7590 03/03/2004

Klarquist Sparkman Campbell
Leigh & Winston LLP
One World Trade Center Suite 1600
121 S W Salmon Street
Portland, OR 97204

EXAMINER

VAUGHAN, MICHAEL R

ART UNIT	PAPER NUMBER
----------	--------------

2131

DATE MAILED: 03/03/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/637,229

Applicant(s)

KOC ET AL.

Examiner

Michael R Vaughan

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 11 August 2000.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☐ Claim(s) _____ is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-21 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 11 August 2000 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- ☒ Notice of References Cited (PTO-892)
- ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 4,5.
- ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- ☐ Notice of Informal Patent Application (PTO-152)
- ☐ Other: _____.

DETAILED ACTION

Claims 1-21 have been examined and are pending.

Specification

Applicant is required to update the status (pending, allowed, etc.) of all parent priority applications in the first line of the specification. The status of all citations of US filed applications in the specification should also be updated where appropriate.

The specification is objected to because of the following: current US patent policy does not permit the use of hyperlinks in the specification. Such links are directed to an Internet site, the contents of which are subject to change without notice. Therefore, the potential for inclusion of new matter would be a constant problem. See pages 10 and 21, for example. Correction is required.

Information Disclosure Statement

An initialed and dated copy of Applicant's IDS form 1449, Paper No. 4,5, is attached to the instant Office action.

Claim Rejections - 35 USC ' 101 Utility

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claim 16 and 17 are rejected under 35 U.S.C. 101 because:

The language of the claim raises a question as to whether the claim is directed merely to an abstract idea that is not tied to a technological art, environment or machine which would result in a practical application producing a concrete, useful, and tangible result to form a the basis of statutory subject matter under 35 U.S.C. 101.

Claims 16 and 17 also rejected under 35 U.S.C. 112, first paragraph. Specifically, since the claimed invention is not supported by either a specific asserted utility or a well established utility for the reasons set forth above, one skilled in the art clearly would not know how to use the claimed invention.

Claim Rejections - 35 USC ' 112, first paragraph

Claims 16 and 17 are rejected under 35 U.S.C. 112, first paragraph, as containing subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention.

Claim Rejections - 35 USC ' 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless --

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

Claims 1, 6, and 12 are rejected under 35 U.S.C. 102(e) as being anticipated by EPS/Solutions, herein EPS (CypherCalc The Cryptographer's Calculator).

As per claim 1, EPS teaches a multiplication module, comprising: a first input and a second input configured to receive a first operand and a second operand,

Art Unit: 2131

respectively, represented as elements of a finite field; an output configured to deliver a Montgomery product of the first operand and the second operand; and a field-select input configured to select multiplication of the first and second operands based on a selected finite field (refer to Montgomery Image and Product calculators).

As per claim 6, EPS teaches A cryptographic processor, comprising: inputs for receiving a first and a second cryptographic parameter represented as elements of a finite field; and a multiplication module configured to receive the cryptographic parameters from the inputs, the multiplication module including processing units configured to determine a Montgomery product of the cryptographic parameters, each processing unit receiving a bit corresponding to the first parameter and partial words of the second parameter (refer to Montgomery Image and Product calculators).

As per claim 12, EPS teaches a dual-field adder, comprising: a first input and a second input situated to receive respective operands; a field-select input; and an addition module, configured to add values supplied to the first and second input according to a value supplied to the field select input (see Description).

Claim Rejections - 35 USC ' 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 2, 3, 4, 8, 9, 10, 11 and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over EPS in view of Brandstrom (USP 4,322,577).

As per claims 2 and 19, EPS teaches his system is for the use of performing calculation based on cryptographical algorithms (refer to Description). EPS teaches the choice of determining which field to compute Montgomery products (see Montgomery Product). EPS fails to explicitly disclose the use of prime fields and binary extension fields. Brandstrom teaches a cryptographical system in which prime fields and binary extension fields are used to carry out the Montgomery multiplications (column 4, lines 40-55 and column 5, lines 20-25). Binary fields and primary fields are well suited to a computer's architecture and cryptographic fundamental security.

In view of this, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of Brandstrom within the system of

EPS because EPS's program allows the user to enter the finite field and Brandstrom teaches finite fields for use on a computer.

As per claim 3, EPS teaches the first operand is processed bit-wise and the second operand is processed word-wise (see Montgomery product).

As per claim 4, EPS teaches the second operand is divided into multiple words that are multiplied with bits of the first operand (see Montgomery product).

As per claim 8, the examiner recites the same rationale for the motivation as recited in the rejection of claim 2 to incorporate the teachings of Brandstrom within the system of EPS.

As per claim 9, EPS teaches the arithmetic operation selectable with the field select input is field addition (see Description).

As per claim 10, EPS teaches a dual-field adder in communication with the field-select input (see Description).

As per claim 11, EPS teaches the first and second cryptographic parameters are represented as m bits and e words of word length w (see Montgomery Products).

Claims 5, 13, 14, and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over EPS in view of Iwamura et al, herein Iwamura, (USP 5,321,752).

As per claims 5 and 13, EPS teaches a dual-field adder that is configurable (see Description). The user supplies the modulus to the arithmetic functions. EPS does not disclose that the addition is executed without carry. Iwamura teaches that in the Galois field, there is no carry bit, which simplifies the hardware (column 18, lines 3-6). Therefore, it would be advantageous to not use a carry bit when operating in the Galois field. In view of this, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of Iwamura within the system of EPS because it would minimize the hardware requirements.

As per claim 14, EPS teaches the addition module includes an exclusive OR gate situated and configured to receive a bit of the first operand and a bit of the second operand (see Description).

As per claim 15, EPS teaches the addition module includes a first and a second exclusive OR gates situated and configured to receive a bit of the first operand and a bit of the second operand, respectively (see Description).

Claims 7 and 16, are rejected under 35 U.S.C. 103(a) as being unpatentable over EPS in view of Monier (USP 5,745,398).

As per claim 7, EPS fails to teach at least one processing unit is configured to communicate intermediate values of partial words of the Montgomery product to a different processing unit. Monier teaches at least one processing unit is configured to communicate intermediate values of partial words of the Montgomery product to a different processing unit as a way of pipelining to increase the performance of the system (column 3, lines 38-67). It would be advantageous to use parallel processing in order to decrease the overall computation time required to execute a calculation. In view of this, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of Monier within the system of EPS because it would decrease the total time needed to solve complication computations.

As per claim 16, EPS teaches a method of determining a Montgomery product of a first cryptographic parameter and a second cryptographic parameter, the method comprising: representing the first cryptographic parameter as a series of bits and representing the second cryptographic parameter as a series of words (see Montgomery Images and Montgomery Products). EPS fails to teach determining an intermediate value of a contribution to the Montgomery product based on a first bit of

Art Unit: 2131

the first cryptographic parameter and the words of the second cryptographic parameter in a first pipeline stage; and determining intermediate values of contributions to the Montgomery product based on remaining bits of the first cryptographic parameter in respective pipeline stages that receive the words of the second cryptographic parameter and an intermediate value from a prior pipeline stage. Monier teaches determining an intermediate value of a contribution to the Montgomery product based on a first bit of the first cryptographic parameter and the words of the second cryptographic parameter in a first pipeline stage; and determining intermediate values of contributions to the Montgomery product based on remaining bits of the first cryptographic parameter in respective pipeline stages that receive the words of the second cryptographic parameter and an intermediate value from a prior pipeline stage (column 3, lines 38-67). Monier teaches at least one processing unit is configured to communicate intermediate values of partial words of the Montgomery product to a different processing unit as a way of pipelining to increase the performance of the system. It would be advantageous to use parallel processing in order to decrease the overall computation time required to execute a calculation. In view of this, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of Monier within the system of EPS because it would decrease the total time needed to solve complication computations.

Claims 17 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over EPS and Monier as applied to claim 16 above, and further in view of Iwamura.

As per claim 17, examiner recites the same rationale for the motivations as recited in the rejection of claims 5 and 13 to incorporate the teachings of Iwamura within the combined system of EPS and Monier.

As per claim 18, EPS teaches a computer-readable medium containing instructions for executing the method of claim 17 (see Description).

Claims 20 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over EPS and Brandstrom as applied to claim 19 above, and further in view of Iwamura.

As per claim 20, examiner recites the same rationale for the motivations as recited in the rejection of claims 5 and 13 to incorporate the teachings of Iwamura within the combined system of EPS and Brandstrom.

As per claim 21, EPS teaches a scalable Montgomery multiplication module situated and configured to obtain a Montgomery product of the first operand and the second operand (see Montgomery Product and Montgomery Image).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael R Vaughan whose telephone number is 703-305-0354. The examiner can normally be reached on M-F 7:30-4:00.


If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MV
Michael R Vaughan

Examiner

Art Unit 2131


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100